(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－296978

(43)公開日　平成11年(1999)10月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00	
Ｇ１１Ｂ　20/12	１０２	Ｇ１１Ｂ　20/12	１０２

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－93276

(22)出願日　平成10年(1998)４月６日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　田中　宏和
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

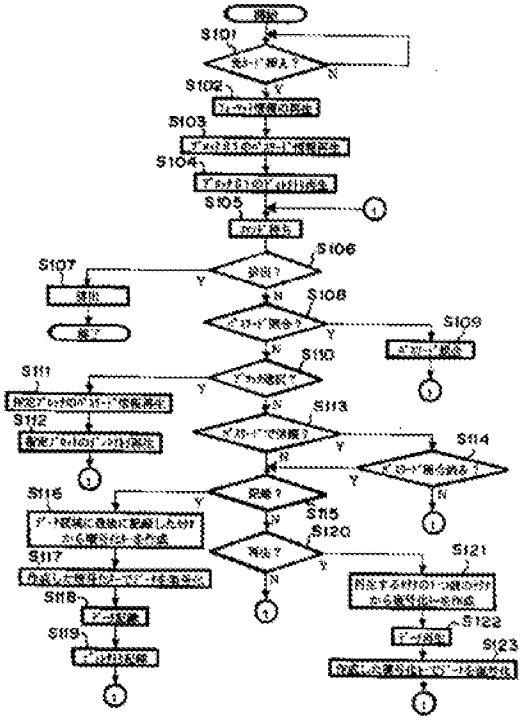
(74)代理人　弁理士　山下　穣平

(54)【発明の名称】　情報記録再生装置

(57)【要約】

【課題】　ファイルごとに暗号化／復号化しているので、１つのキーが特定されてしまうとファイル全体が解読されてしまう。

【解決手段】　セクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタに記録されているデータをもとに暗号化キー／復号化キーを作成する。また、所定の数をファイルのディレクトリに記録し、ファイルごとに所定の数を異ならせる。



【特許請求の範囲】
【請求項１】　１つまたは複数のセクタより成る複数のトラックを有する追記型記録媒体にデータを記録／再生する手段と、前記記録媒体にデータを管理するためのディレクトリを記録／再生する手段と、データの記録前にデータを暗号化する手段と、再生されたデータを復号化する手段とを有する情報記録再生装置において、前記記録媒体に既に記録されているデータをもとにデータを暗号化／復号化するための暗号化キー／復号化キーを作成する手段を備え、前記暗号化キー／復号化キー作成手段はセクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタに記録されているデータをもとに暗号化キー／復号化キーを作成することを特徴とする情報記録再生装置。
【請求項２】　前記暗号化キー／復号化キー作成手段は、前記所定の数だけ前のセクタにデータが記録されていないときは、予め決められたデフォルト値をもとに暗号化キー／復号化キーを作成することを特徴とする請求項１に記載の情報記録再生装置。
【請求項３】　前記所定の数を前記ディレクトリに記録しておくことを特徴とする請求項１に記載の情報記録再生装置。
【請求項４】　前記記録媒体のファイルごとに前記ディレクトリに記録する所定の数を異ならせることを特徴とする請求項３に記載の情報記録再生装置。
【請求項５】　前記記録媒体は、光カードであることを特徴とする請求項１に記載の情報記録再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報記録媒体に情報を記録／再生する情報記録再生装置に関し、特にデータの暗号化／復号化に関するものである。
【０００２】
【従来の技術】従来、光学的に情報を記録し、あるいは記録された情報を読みだす媒体の形態として、ディスク状、カード状、テープ状等各種のものが知られている。これらの媒体のうち、カード状に形成された光学的情報記録媒体（以下光カードと称する）は、磁気カードと比較して数千倍～一万倍の記録容量を有し、光ディスクと同様に書き換えはできないが、その記録容量が１～６Ｍバイトと大きいことから銀行の預金通帳、携帯用の地図、あるいは買い物等に用いるプリペイドカード等として広い応用範囲が考えられている。
【０００３】このような光カードにデータを記録、再生する場合、通常は、データと共にデータを管理するためのディレクトリを光カードの一部に記録して、データをファイルごとに管理するのが一般的である。ディレクトリは図３に示すようにファイル名、先頭データの開始アドレス、連続して記録したセクタ数等のファイル管理に必要な情報から成っている。このディレクトリはデータを記録する度にデータの管理情報として光カードの記録領域の一部に記録される。
【０００４】図４は光カードの概略平面図で、１は光カード、２は情報記録領域である。情報記録領域２内にはトラッキングトラック３１ ～３n+1 が一定間隔を置いて平行に配列され、その各トラッキングトラックの間に情報を記録するための情報トラック４１ ～４n が設けられている。各情報トラックの両端には情報トラックを識別するための物理トラックナンバー５１ ～５n が予め付加されている。また、図４の光カードでは、情報トラック４２ ～４k をブロック６１ 、情報トラック４k+1 ～４n-1 をブロック６２ として、情報記録領域２が２つのブロックに分割されている。光カード１を複数のブロックに分割することに関しては特開昭６３－２４４３８５号公報に記載されている。
【０００５】例えば、光カードを医療情報記録用の媒体として用い、これにある患者の心電図情報と血圧情報を記録する時は、ブロック６１ に心電図情報を、ブロック６２に血圧情報を記録することが可能である。このように記録するデータの種類ごとにブロック分けを行った場合、心電図情報を再生する時はブロック６１ 内のデータだけを再生すればよいために、アクセス時間を短縮することができる。もちろん、ブロックの分割数やブロック内の情報トラック数は記録するデータの種類やデータ量に応じて任意に設定することができる。
【０００６】また、光カード１においては、ブロックごとに１本の情報トラックのセクタ数とセクタサイズを変える方式が知られている。図５は１本の情報トラックに記録するデータのセクタサイズとセクタ数の関係の例を示している。図５において、セクタタイプ１は１０２４バイトのセクタを情報トラック４に１個記録し、セクタタイプ２は５１２バイトのセクタを情報トラック４に２個記録し、セクタタイプ３は２５６バイトのセクタを情報トラック４に４個記録し、セクタタイプ４は１２８バイトのセクタを情報トラック４に６個記録し、セクタタイプ５は６４バイトのセクタを情報トラック４に８個記録し、セクタタイプ６は３２バイトのセクタを情報トラック４に１２個記録する事を示している。
【０００７】このような方式で、例えば７６８バイトのデータをセクタタイプ１で記録する場合は、１セクタ（情報トラック１本）を記録するだけでよいが、セクタタイプ６で記録すると、２４セクタ（情報トラック２本）を記録しなければならない。そのため、セクタタイプ６で記録した場合は時間がかかるばかりでなく、光カードの記録容量を無駄にしてしまう。また、３２バイトのデータをセクタタイプ１で記録する場合は、１本の情報トラックを使ってしまうが、セクタタイプ６で記録すると、１セクタで済み、セクタタイプ１に比べて１／１２の情報トラックしか使わない。このように記録するデータサイズに応じてセクタタイプを選択することによ

り、アクセス速度を早くできるばかりでなく、光カードの記録領域を有効に使用することができる。

【０００８】ここで、図４において、７１1～７１iはブロック６１内に記録されているデータ、７２1～７２jはブロック６２内に記録されているデータである。８１1～８１iはブロック６１内に記録されているデータ７１を管理するためのディレクトリ、８２1～８２jはブロック６２内に記録されているデータ７２を管理するためのディレクトリである。データはＢ方向に追記し、ディレクトリはＦ方向に追記していく。前述のように光カードに医療情報を記録する場合は、心電図情報をデータ７１、その管理情報をディレクトリ８１、血圧情報を７２、その管理情報を８２として記録すればよい。

【０００９】また、心電図情報のようにデータ量の大きな情報を記録する場合は、データ７１1～７１iのようにセクタサイズを大きくし、１本の情報トラックに記録するセクタ数を１つにすると、アクセス速度を早めることができる。逆に、血圧情報のようにデータ量が小さい場合は、データ７２1～７２jのようにセクタサイズを小さくし、１本の情報トラックに記録するセクタ数を多くすれば、光カードの記録容量を有効に使用することができる。なお、ディレクトリのデータサイズは比較的小さいので、例えばセクタタイプ５で記録するのがよい。

【００１０】更に、光カードのいずれのブロックにも属さない情報トラック４1 と情報トラック４n には、上述した光カード１のブロック分割数、各ブロックのトラック本数、各ブロックで使用するセクタタイプ等の光カード管理情報９（以下、フォーマット情報と称する）が記録されている。図６はこのフォーマット情報の内容を示す図で、先頭の識別情報はフォーマット情報であることを示す情報であり、例えばＡＳＣＩＩコードで〝ＦＭＴ〟といった情報が記録される。次のブロック分割数は光カード１がいくつのブロックに分割されているかを示す情報である。次に、ブロック61 ～ブロック６n の各情報トラック数とセクタタイプを示す情報が記録されている。

【００１１】ところで、光カードの情報の記録や再生は任意の使用者が行うことが可能である。そのため、多数の使用者が使用することにより誤って必要な情報を破壊してしまったり、故意に情報を改ざんしたり、あるいは機密性の高い情報を他人に見られてしまう可能性がある。そこで、光カードのブロックごとに個人固有の情報（以下パスワード情報と称する）を記録しておき、パスワード情報が記録されているブロック内にデータを記録または再生する時は、パスワード情報を入力し、入力したパスワード情報とブロック内に記録されているパスワード情報とを照合し、照合結果が一致した時のみブロック内の情報の記録再生を許可するという方法が採用されている。

【００１２】図４の１０１1と１０１2はブロック６１のパスワード情報である。このパスワード情報は、図７に示すように識別情報とパスワード情報から構成されている。識別情報はパスワード情報であることを示す情報で、例えば、ＡＳＣＩＩコードで〝ＰＷＤ〟といった情報が用いられる。次に、実際のパスワード情報が記録される。このようなパスワード情報を用いることにより、例えば、心電図情報を記録再生する場合は、ホストコンピュータからパスワード情報を入力し、これがブロック６１内のパスワード情報と一致した時のみ心電図情報のアクセスが可能となる。これに対して、ブロック６２内のパスワードを記録するトラック４k+1 、４n-1 にはパスワード情報が記録されていないため、自由に血圧情報の記録再生が可能である。

【００１３】しかし、光カードに情報を記録する場合は、微小スポット状に絞られた光ビームを記録情報に従って変調し、変調された光ビームを情報トラック上にスキャンすることにより、光学的に検出可能なビット列として記録するので、パスワードでブロック６内のアクセスを制限しても、光学顕微鏡等を用いて解析されると機密性の高い情報が他人に見られてしまう可能性がある。そこで、更にセキュリティーを高めるために、光カードに記録するデータを暗号化キーにより暗号化して記録し、再生時は暗号化されたデータを復号化キーにより復号化して再生する方法が提案されている。

【００１４】この方式を用いることにより、光カードに記録されたデータを光学顕微鏡等によって解析された場合でも、解析したデータが意味をなさないものとなり、光カードに記録されたデータの機密性を保つことが出来る。光カードに記録するデータを暗号化する方式としては、様々な方式が考えられ、公開鍵方式のＲＳＡ暗号や共通鍵方式のＤＥＳ暗号などが有名であるが、ここでは、説明を簡単にするためにシーザ暗号を例に説明する。シーザ暗号ではアルファベットに数をＡ＝０、Ｂ＝１、…、Ｚ＝２５と対応させ、平文の１文字を表す数をｘ、暗号文の１文字を表す数をｃ、暗号化キーを表す数をｋとおくと、

ｃ＝（ｘ＋ｋ）ｍｏｄ　２６

の関係式で表される暗号方式である。但し、ａ　ｍｏｄ　ｎはａをｎで割った余りを示す。また、暗号文を平文にする復号化の場合は、

ｘ＝（ｃ－ｋ）ｍｏｄ　２６

の関係式で表される。従って、シーザ暗号では暗号化キーと復号化キーは同じキーとなる。そして、例えば暗号化キーｋが１の場合は、平文が〝ＡＢＣ〟であれば暗号文は〝ＢＣＤ〟と暗号化される。しかしながら、このままではアルファベットの文字しか扱う事が出来ないので、暗号化の式を、

ｃ＝（ｘ＋ｋ）ｍｏｄ　２５６

の様に拡張し、また復号化の式を、

ｘ＝（ｃ－ｋ）ｍｏｄ　２５６

の様に拡張することにより、１バイトで表される全ての文字を扱うことが可能となる。そして、これらの暗号化または復号化は高速で実行する事が望ましいために、ハードウェアで行うのが一般的である。

【００１５】次に、暗号化キーの作成方法について説明する。暗号化キーの作成方法は様々な方法が考えられるが、例えば光カードに記録されているフォーマット情報、パスワード情報、ディレクトリ等の情報をある関数に入力する事により暗号化キーを作成できる。従って、暗号化キーをｋ、キーを作成するための暗証番号をｎとすると、

ｋ＝Ｆ（ｎ）

の関係式がなりたつ。但し、関数Ｆ（ｎ）は暗号化キーを作成する関数であり、圧縮関数等が用いられる。圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。光カード情報記録再生装置はこの暗号化キーを用いてデータの暗号化、暗号化されたデータの復号化を行う。

【００１６】次に、光カードに情報を記録または再生する光カード情報記録再生装置について説明する。図８は光カード情報記録再生装置の概略構成を示すブロック図である。図８において、３１は光カード１に情報を記録、再生する光カード情報記録再生装置であり、上位制御装置のホストコンピュータ３２に接続されている。情報記録再生装置３１はホストコンピュータ３２の制御に基づいて情報の記録、再生を行う。３７は不図示の搬送機構を駆動して光カード１を情報記録再生装置３１内の所定位置に導入し、また、所定位置にて光カード１をＲ方向に往復移動させ、更に光カード１を機外に排出するためのカード送りモータである。３８は光源の半導体レーザを含む光ビーム照射光学系であり、情報の記録、再生時には光源の光ビームを微小光スポットに絞って光カード１上に照射する。

【００１７】また、３９は光カード１から反射された光を検出する光検出器、４０は光ビーム照射光学系３８の一部を駆動して光カード１面上の光スポットのピント位置をＺ方向、即ち光カード面と垂直方向に移動させてオートフォーカス制御を行うためのＡＦアクチュエータ、４１は光ビーム照射光学系３８の一部を駆動して光カード１面上の光スポットをＹ方向、即ち光カードの情報トラックに直交する方向に移動させてオートトラッキング制御を行うためのＡＴアクチュエータである。これらの光ビーム照射光学系３８、光検出器３９、ＡＦアクチュエータ４０、ＡＴアクチュエータ４１を含んで光ヘッド３０が構成されている。３６は光ヘッド５０をＹ方向に移動させて光スポットを所望のトラックにアクセスするためのヘッド送りモータである。

【００１８】ＭＰＵ３３は情報記録再生装置３１内の各部を制御するためのプロセッサ回路であってＲＯＭ、ＲＡＭを内蔵している。ＭＰＵ３３はヘッド送りモータ３６、カード送りモータ３７などを制御し、また、ホストコンピュータ３２とデータの送受信を行う。ＡＴ／ＡＦ制御回路３４は光検出器３９からの出力信号からＡＴ／ＡＦ制御信号を検出し、それに基づいてＡＦアクチュエータ４０とＡＴアクチュエータ４１を駆動し、光ビーム照射光学系３８からの光スポットがカード面に焦点を結ぶように、光スポットが情報トラックに追従して走査するようにオートフォーカス制御とオートトラッキング制御を行う。

【００１９】変復調回路３５はＭＰＵ３３の制御に基づいて記録データを変調し、再生データを復調するための回路、暗号化／復号化回路４２は記録データを暗号化し、再生データを復号化するための回路である。情報の記録時には、ホストコンピュータ３２からＭＰＵ３３に記録データが転送され、その後、暗号化／復号化回路４２で記録データが暗号化される。変復調回路３５では暗号化されたデータを変調し、変調信号に従って光ビーム照射光学系３８内の光源を駆動し、この変調された光源の光ビームを光カード１の情報トラックに走査することによって情報の記録を行う。

【００２０】一方、情報の再生時には、光ビーム照射光学系３８から再生用光ビームを光カード１の情報トラックに走査し、光検出器３９で光カード１からの反射光を検出する。このとき、変復調回路３５は光検出器３９の出力信号から情報再生信号を生成し、再生信号の復調を行う。復調されたデータはＭＰＵ３３のＲＡＭに蓄えられ、その後、暗号化／復号化回路４２によって暗号化されたデータが復号化される。復号化されたデータはＭＰＵ３３からホストコンピュータ３２に転送される。ホストコンピュータ３２は情報記録再生装置３１とコマンドやデータの送受信を行い、セクタごとに情報の記録や再生を行う。

【００２１】次に、光カード情報記録再生装置において光カードのデータにアクセスする際の動作について図９を参照して説明する。図９において、まず、情報記録再生装置３１は光カード１が挿入されたかを監視している（Ｓ９０１）。光カードが挿入されると、初めにフォーマット情報９を再生する（Ｓ９０２）。フォーマット情報を再生すると、光カード１の記録領域がどのように分割されているかが分かる。この場合、フォーマット情報に基づいてデフォルトのブロックとしてブロック６１が自動的に選択され、ブロック６１のパスワード情報１０１が再生される（Ｓ９０３）。パスワード情報はＭＰＵ３３内のＲＡＭに記憶し、もし、パスワードが記録されていなかったらこのブロックがパスワードで保護されていないことをＲＡＭに記憶しておく。

【００２２】次いで、ブロック６１のディレクトリ８１を順次再生し、ＭＰＵ３３内のＲＡＭに読み込んだ順に記憶する（Ｓ９０４）。光カード１には、データもディレクトリもシーケンシャルに記録されているので、ディ

レクトリを再生すると、再生したディレクトリの数と、再生したディレクトリの内容から、ディレクトリの記録開始位置とデータの記録開始位置が求まる。このようにして光カード情報記録再生装置３１はホストコンピュータ３２からのコマンドを待つ状態となり（Ｓ９０５）、コマンドの種類に応じて以下の処理を実行する。まず、コマンドが排出コマンドであるかをチェックする（Ｓ９０６）。コマンドが排出コマンドであった場合は、光カード１の排出を実行し、この光カード１に対する処理を終了する（Ｓ９０７）。

【００２３】一方、コマンドが排出コマンドでなかった場合は、パスワード照合コマンドであるかどうかをチェックし（Ｓ９０８）、もし、パスワード照合コマンドであった場合は、パスワードの照合を行う（Ｓ９０９）。即ち、Ｓ９０３で再生してＲＡＭに記憶しておいたパスワードと、パスワード照合コマンドによってホストコンピュータ３２から送られてきたパスワードを照合する。ここで、もし両方のパスワードが一致した場合は、ブロック６１におけるパスワードが照合済みであることをＭＰＵ３３内のＲＡＭに記憶しておく。パスワードが一致しなかった場合は、そのままＳ９０５のコマンド待ち処理に移行する。また、現在選択されているブロックがパスワードで保護されていないときは、照合は行わず、Ｓ９０５に戻る。

【００２４】パスワードの照合処理を終了すると、コマンドがブロック選択コマンドであるかをチェックし（Ｓ９１０）、ブロック選択コマンドであった場合は、Ｓ９０２で再生したフォーマット情報に基づいて指定されたブロックのパスワード情報を再生する（Ｓ９１１）。再生したパスワード情報はＳ９０３と同様にＭＰＵ内のＲＡＭに記憶しておく。次いで、指定されたブロックに記録されているディレクトリをすべて再生し（Ｓ９１２）、ＭＰＵ３３内のＲＡＭに読み込んだ順に記憶し、ブロック選択の処理を終了する。

【００２５】一方、Ｓ９１０でコマンドがブロック選択コマンドでなかった場合は、コマンドは記録コマンドか再生コマンドであり、現在選択されているブロックがパスワードで保護されている場合は、パスワードが照合済みか確かめなければならないので、まず、パスワードで保護されているか調べ（Ｓ９１３）、保護されている場合はパスワードが照合済みかをチェックする（Ｓ９１４）。このチェックは、Ｓ９０９でＲＡＭに記憶しておいた情報を参照することによって行う。パスワードが照合済みでない場合は、Ｓ９０５に戻る。パスワードが照合済みの場合、及びＳ９１３においてパスワードで保護されていないと判断された場合は、次のＳ９１５の処理に移行する。

【００２６】Ｓ９１５においては、コマンドが記録コマンドであるかをチェックし、記録コマンドであった場合は、暗号化に必要な暗号化キーを作成する（Ｓ９１６）。暗号化キーは、ＲＡＭに記憶されている最後のディレクトリを基に作成する。このディレクトリは、現在アクセスしているブロックに最後に記録されたディレクトリである。このブロックに初めて記録するデータである場合は、まだ、このブロックにはディレクトリは記録されていないので、予め決められたデフォルトの値を基に暗号化キーを作成する。暗号化キーの作成には、前述のような圧縮関数が用いられる。

【００２７】次いで、記録コマンドと共にホストコンピュータ３２から送られてきたデータをＳ９１６でディレクトリから作成した暗号化キーによって暗号化し（Ｓ９１７）、暗号化されたデータを現在選択されているブロックの記録を開始すべき位置から記録する（Ｓ９１８）。その後、記録したデータを管理するためのディレクトリを記録し、ＲＡＭにも同様のディレクトリを記憶して（Ｓ９１９）、記録コマンドの処理を終了する。

【００２８】一方、Ｓ９１５で記録コマンドでなかった場合は、コマンドが再生コマンドであるかをチェックする（Ｓ９２０）。再生コマンドでない場合は、情報記録再生装置３１がサポートしないコマンドなので、Ｓ９０５に戻り、再生コマンドであった場合は、復号化キーを作成する（Ｓ９２１）。復号化キーはＲＡＭに記憶されているディレクトリから再生すべきデータのディレクトリをサーチし、そのディレクトリの１つ前のディレクトリを基に作成する。１つ前のディレクトリが無い場合は、予め決められたデフォルトの値を基に復号化キーを作成する。次いで記録コマンドで指定されたファイル名と、ＲＡＭに記憶しているディレクトリから再生すべきセクタアドレスを求め、データを再生する（Ｓ９２２）。ここで再生したデータは、暗号化されたデータであるので、作成した復号化キーを用いて復号化し（Ｓ９２３）、復号化したデータをホストコンピュータ３２に転送して再生処理を終了する。

【００２９】

【発明が解決しようとする課題】従来の方法では、最後に記録したファイルのディレクトリから暗号化キーを作成し、再生するファイルの１つ前のファイルのディレクトリから復号化キーを作成している。即ち、ファイルごとに暗号化／復号化しているので、１つのキーが特定されてしまうと、ファイル全体が解読されてしまい、セキュリティーが低いという問題点があった。

【００３０】本発明は、上記従来の問題点に鑑み、セクタごとに暗号化キー／復号化キーを異ならせることにより、更にセキュリティーを向上することが可能な情報記録再生装置を提供することを目的とする。

【００３１】

【課題を解決するための手段】本発明の目的は、１つまたは複数のセクタより成る複数のトラックを有する追記型記録媒体にデータを記録／再生する手段と、前記記録媒体にデータを管理するためのディレクトリを記録／再

生する手段と、データの記録前にデータを暗号化する手段と、再生されたデータを復号化する手段とを有する情報記録再生装置において、前記記録媒体に既に記録されているデータをもとにデータを暗号化／復号化するための暗号化キー／復号化キーを作成する手段を備え、前記暗号化キー／復号化キー作成手段はセクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタに記録されているデータをもとに暗号化キー／復号化キーを作成することを特徴とする情報記録再生装置によって達成される。

【００３２】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。まず、本発明の第１の実施形態について説明する。第１の実施形態による情報記録再生装置のハードウェアの構成は図８と同様の構成とし、記録媒体としては図４の光カードを用いるものとする。また、光カード１に記録するファイルデータを管理するためのディレクトリは図３、セクタタイプは図５、フォーマット情報は図６、パスワード情報は図７のものを用いるものとする。これらの図８、図４、図３、図５、図６、図７については先に述べたので詳しい説明を省略する。

【００３３】図１は本実施形態の動作を示すフローチャートである。なお、図１のＳ１０１～Ｓ１１５は従来の動作を示す図９のＳ９０１～Ｓ９１５と同じであるので簡単に説明する。図９において、まず、Ｓ１０１で情報記録再生装置３１に光カード１が挿入されると、光カード１のフォーマット情報を再生する（Ｓ１０２）。フォーマット情報を再生すると、光カード１のブロックの分割状態が分かり、本実施形態では従来と同様にデフォルトのブロックとしてブロック６１を自動的に選択し、ブロック６１のパスワード情報を再生する（Ｓ１０３）。パスワード情報はＭＰＵ３３内のＲＡＭに記憶しておく。もし、パスワード情報が記録されていなかったときはこのブロックがパスワードで保護されていないことをＲＡＭに記憶しておく。

【００３４】次いで、ブロック61 のディレクトリ81を順次再生し（Ｓ１０４）、ＭＰＵ３３内のＲＡＭに読み込んだ順に記憶し、光カードにはデータもディレクトリもシーケンシャルに記録されているので、再生したディレクトリの数と内容からディレクトリの記録開始位置とデータの記録開始位置が得られる。次に、情報記録再生装置３１はホストコンピュータ３２からのコマンドを待ち（Ｓ１０５）、コマンドの種類に応じて以下の処理を実行する。まず、コマンドが排出コマンドであるかをチェックし（Ｓ１０６）、コマンドが排出コマンドであれば光カード１を排出し、この光カードに対する処理を終了する（Ｓ１０７）。排出コマンドでなかったときは、パスワード照合コマンドであるかをチェック（Ｓ１０８）、パスワード照合コマンドであったときはパスワードの照合を行う（Ｓ１０９）。即ち、ＲＡＭに記憶しておいたパスワードとパスワード照合コマンドによってホストコンピュータ２２から送られてきたパスワードを照合し、両方のパスワードが一致すると、ブロック６１におけるパスワードが照合済みであることをＭＰＵ３３内のＲＡＭに記憶しておく。パスワードが一致しなかったときは、Ｓ１０５のコマンド待ち処理に移行する。

【００３５】一方、Ｓ１０８でパスワード照合コマンドでなかったときはブロック選択コマンドであるかをチェックし（Ｓ１１０）。ブロック選択コマンドであれば、Ｓ１０２で再生したフォーマット情報に基づいて指定されたブロックのパスワード情報を再生する（Ｓ１１１）。パスワード情報は同様にＲＡＭに記憶しておく。次いで、指定されたブロックのディレクトリを全て再生し（Ｓ１１２）、同様にＲＡＭに読み込んだ順に記憶してブロック選択の処理を終了する。また、ブロック選択コマンドではなかったときはコマンドは記録コマンドか再生コマンドであり、現在選択されているブロックがパスワードで保護されている場合は、パスワードが照合済みか確かめなければならないので、まず、パスワードで保護されているか調べ（Ｓ１１３）、保護されている場合はパスワードが照合済みかをチェックする（Ｓ１１４）。これは、ＲＡＭに記憶しておいた情報を参照することによって行う。パスワードが照合済みでなかったときはＳ１０５に戻り、パスワードが照合済みの場合、Ｓ１１３でパスワードで保護されていなかったときは次のＳ１１５に移行する。

【００３６】Ｓ１１５ではコマンドが記録コマンドであるかをチェックし、記録コマンドであった場合は、暗号化に必要な暗号化キーを作成する（Ｓ１１６）。本実施形態では、これから記録するセクタより所定の数だけ前のセクタのデータを暗証番号として暗号化キーを作成し、例えば、ここでは１つ前のセクタのデータから暗号化キーを作成している。また、暗号化キーを作成するための圧縮関数はどのようなものでもよいが、例えば、１つ前のセクタの全てのバイトを排他的論理和で加算した１バイトの値を暗号化キーとする。暗号化キーはＭＰＵ３３によって作成している。

【００３７】従って、ＭＰＵ３３はこれから記録するセクタの１つ前のセクタに記録されているデータを再生し、そのデータをもとに暗号化キーを作成する。なお、このデータは現在アクセスしているブロックに最後に記録されたデータであり、このブロックに初めてデータを記録する場合は、まだ、このブロックにはデータは記録されていないので、予め決められたデフォルトの値をもとに暗号化キーを作成する。暗号化キーを作成すると、記録コマンドと共にホストコンピュータ３２から送られてきたデータを暗号化／復号化回路４２によってＳ１１６で作成した暗号化キーによって暗号化する（Ｓ１１７）。次いで、暗号化されたデータを現在選択されてい

るブロックの記録開始位置から記録する（Ｓ１１８）。Ｓ１１６からＳ１１８の処理は記録するセクタごとに繰り返し行い、セクタごとに１つの前のセクタのデータをもとに暗号化キーを作成し、セクタごとに作成した暗号化キーを用いて暗号化することによって記録していく。その後、記録したデータを管理するディレクトリを記録し、ＲＡＭにも同様のディレクトリを記憶して記録コマンドの処理を終了する（Ｓ１１９）。

【００３８】次に、Ｓ１１５で記録コマンドでなかったときは、コマンドが再生コマンドであるかチェックし（Ｓ１２０）、再生コマンドでない場合は、情報記録再生装置３１がサポートしないコマンドなのでＳ１０５に戻る。再生コマンドであった場合は、復号化キーを作成する（Ｓ１２１）。本実施形態では、復号化キーを作成する場合、再生コマンドで指定されたファイル名と、ＲＡＭに記憶しているディレクトリから再生すべきセクタアドレスを求め、次いで再生するセクタの所定の数だけ前のセクタに記録されているデータを再生し、そのデータを基に復号化キーを作成している。復号化キーはＭＰＵ３３によって作成し、また、ここでは、例えば再生するセクタの１つ前のセクタに記録されているデータをもとに復号化キーを作成している。１つ前のセクタが無い場合は、予め決められたデフォルトの値を基に復号化キーを作成する。

【００３９】復号化キーを作成すると、データを再生し（Ｓ１２２）、ここで再生したデータは暗号化されたデータであるので、暗号化／復号化回路４２により作成した復号化キーを用いてデータを復号化し、復号化したデータをホストコンピュータ３２に転送する（Ｓ１２３）。Ｓ１２１～Ｓ１２３の処理は再生するセクタごとに繰り返し行い、セクタごとに１つ前のセクタのデータをもとに復号化キーを作成してデータを再生していく。ホストコンピュータ３２から指示されたすべてのセクタを再生すると、再びＳ１０５に戻ってコマンドを待つ状態となる。

【００４０】このように本実施形態では、これから記録／再生するデータの暗号化キー／復号化キーを所定の数け前のセクタに記録されているデータをもとに作成しているので、セクタごとに暗号化キー／復号化キーが異なり、仮にあるセクタの暗号化キー／復号化キー見破られたとしても、他のセクタを解読することはできず、従来に比べて大幅にセキュリティーを高めることができる。更に、暗号化キーや復号化キーを作成するためのデータは暗証番号として記録されたものではないため、暗証番号であるとは気付かれにくく、記録領域が解析されたとしても暗証番号を特定しにくい利点がある。

【００４１】次に、本発明の第２の実施形態について説明する。第１の実施形態では暗号化キーと復号化キーを作成する場合、記録または再生するセクタのいくつ前のセクタのデータをもとに作成するかを固定としているが、本実施形態ではそれをファイルごとに変えている。具体的には、図２のディレクトリを用い、ディレクトリの中にいくつ前のセクタのデータを暗号化キーと復号化キーを作成するかを示す所定の数値を記録しておく。この所定の値は、情報記録再生装置３１またはホストコンピュータ３２によってファイルごとにデータを記録する際に任意の値を選択して記録するものとする。

【００４２】本実施形態の動作は図１と同様であるが、Ｓ１１５で記録コマンドと判断したきは、既にＲＡＭに読み込まれているディレクトリ、即ち、記録するファイルのディレクトリに含まれている所定の値を参照し、記録するセクタより所定の値だけ前のセクタに記録されているデータをもとに暗号化キーを作成する（Ｓ１１６）。次いで、作成した暗号化キーを用いてデータを暗号化し（Ｓ１１７）、光カード１に記録する（Ｓ１１８）。Ｓ１１６～Ｓ１１７の処理はセクタごとに繰り返し行い、セクタごとに記録するセクタより所定の値だけ前のセクタのデータをもとに暗号化キーを作成し、データを記録していく。ホストコンピュータ３２から指示されたすべてのセクタを記録すると、記録データを管理するためのディレクトリを記録して（Ｓ１１９）、記録処理を終了する。なお、ファイルを始めて記録するときは情報記録再生装置３１またはホストコンピュータ３２で所定の値を決め、その値を用いて暗号化キーを作成し、ディレクトリを記録するときに所定の値を含むディレクトリを記録する。

【００４３】一方、Ｓ１２０で再生コマンドと判断したときはホストコンピュータ３２から指定されたファイル名を有するディレクトリ（既にＲＡＭに読み込まれている）に含まれている所定の値を参照し、その値を用いて再生するセクタより所定の値だけ前のセクタに記録されているデータをもとに復号化キーを作成する（Ｓ１２１）。次いで、Ｓ１２２でデータを再生し、Ｓ１２３で復号化キーを用いてデータを復号化する。Ｓ１２１～Ｓ１２３の処理はセクタごとに繰り返し行い、セクタごとに所定の値だけ前のセクタのデータをもとに復号化キーを作成し、データを再生していく、ホストコンピュータ３２から指示されたすべてのセクタを再生すると、再びＳ１０５に戻ってコマンドを待つ状態となる。

【００４４】本実施形態においては、ディレクトリに所定の値を記録し、その値を用いて暗号化キーと復号化キーを作成しているので、暗号化キーと復号化キーを記録または再生するセクタよりいくつ前のセクタのデータをもとに作成するかをファイルごと変えることができ、第１の実施形態に比べて更にセキュリティーを高めることができる。

【００４５】なお、以上の実施形態では、暗号化アルゴリズムとしてシーザ暗号を用いているが、ＤＥＳ等の他の暗号化アルゴリズムを用いてもよい。特に、ＤＥＳはシーザ暗号よりも複雑で解読しにくいので、よりセキュ

リティーを高めることができる。また、情報記録媒体としては光カードに限らず、追記型の記録媒体であればどのような媒体を用いてもよい。

【００４６】

【発明の効果】以上説明したように本発明によれば、セクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタのデータをもとに暗号化／復号化キーを作成することにより、セクタごとに異なる暗号化キー／復号化キーを用いてデータを暗号化／復号化することができ、仮に１つのセクタのキーが特定されても、他のセクタは解読することができず、従来に比べてセキュリティーを大幅に向上することができる。また、データは暗証番号として記録されたものではないため、暗証番号であるとは気付かれにくく、記録領域が解析されても暗証番号を特定しにくくなり、また、暗証番号をデータとは別にデータ領域に記録する必要はないので、その分記録領域を有効に使用することができる。更に、所定の数をディレクトリに記録し、ファイルごとにその値を異ならせることにより、更にセキュリティーを向上することができる。

【図面の簡単な説明】

【図１】本発明による情報記録再生装置の第１の実施形態の動作を示すフローチャートである。

【図２】本発明の第２の実施形態に用いるディレクトリを示す図である。

【図３】従来例のディレクトリを示す図である。

【図４】光カードの例を示す図である。

【図５】セクタタイプの例を示す図である。

【図６】フォーマッド情報の例を示す図である。

【図７】パスワード情報の例を示す図である。

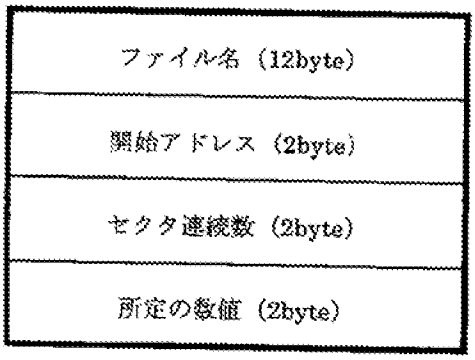
【図８】光カード情報記録再生装置の例を示す図である。

【図９】図８の装置の光カードにアクセスする動作を示すフローチャートである。

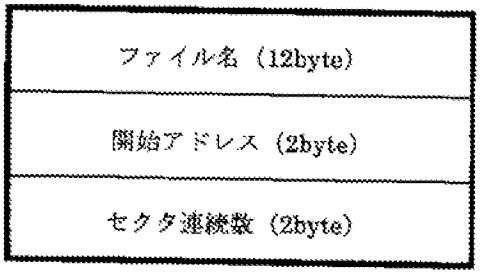
【符号の説明】

１　光カード
２　記録領域
４　情報トラック
６　ブロック
７　データ
８　ディレクトリ
９　フォーマット情報
１０　パスワード
３１　光カード情報記録再生装置
３２　ホストコンピュータ
３３　ＭＰＵ
３４　ＡＴ／ＡＦ制御回路
３８　光ビーム照射光学系
４２　暗号化／復号化回路

【図２】



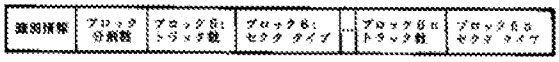
【図３】



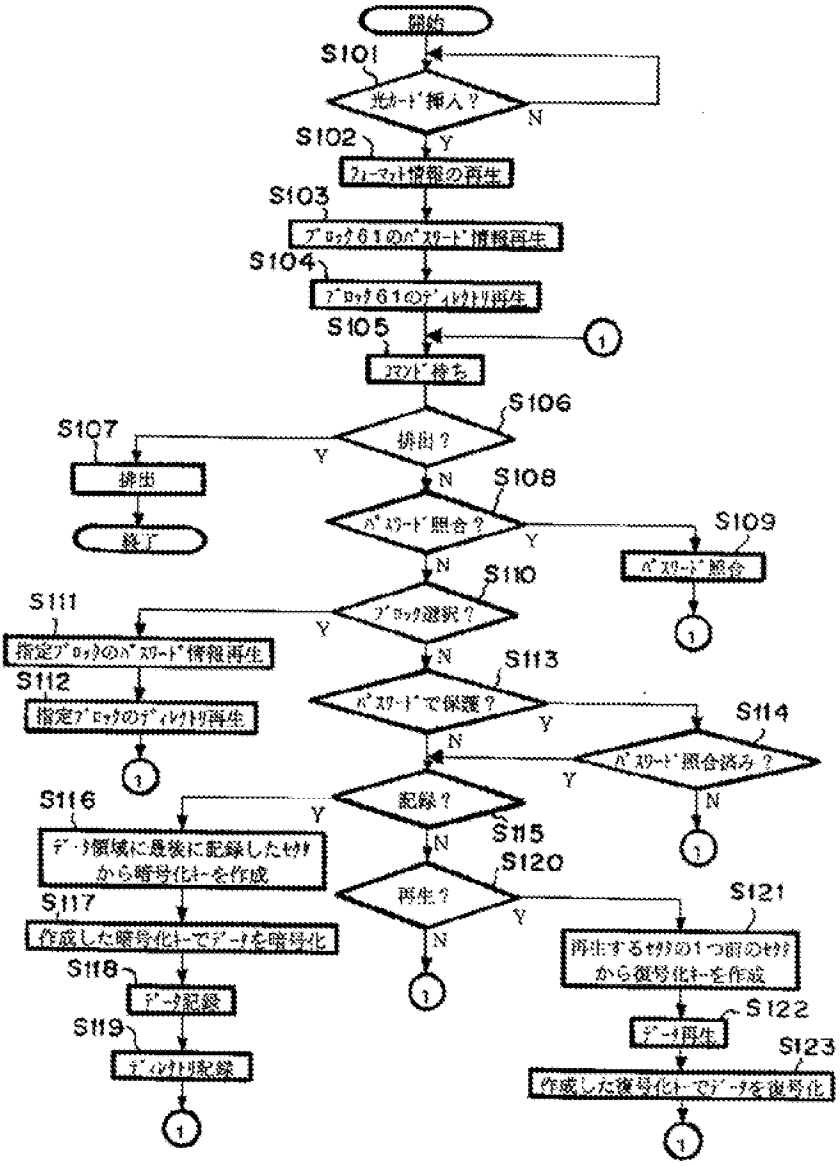
【図５】

セクタ タイプ	セクタ数	セクタサイズ（バイト）
セクタ タイプ１	1	1024
セクタ タイプ２	2	512
セクタ タイプ３	4	256
セクタ タイプ４	6	128
セクタ タイプ５	8	64
セクタ タイプ６	12	32

【図６】



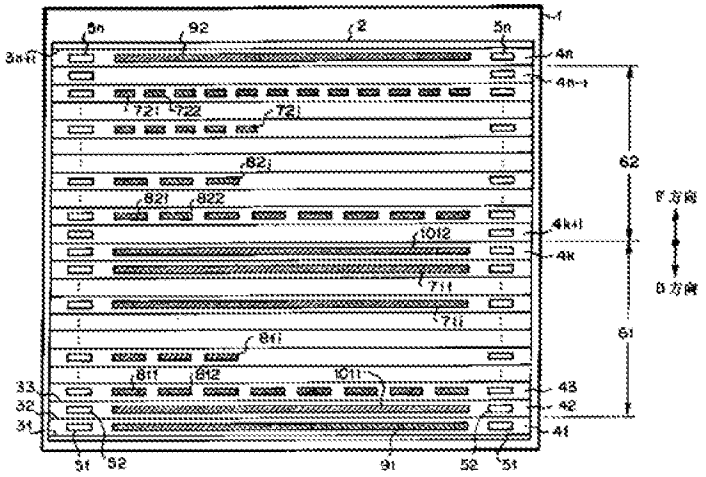
【図1】



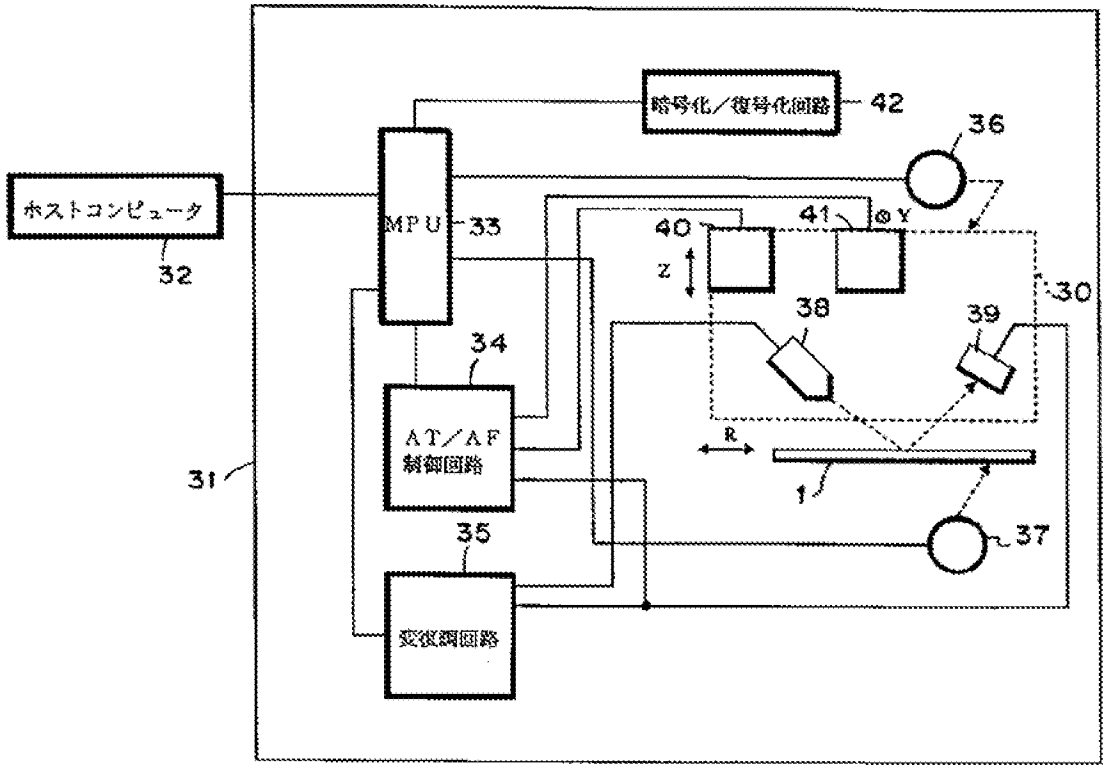
【図7】

識別情報	パスワード情報

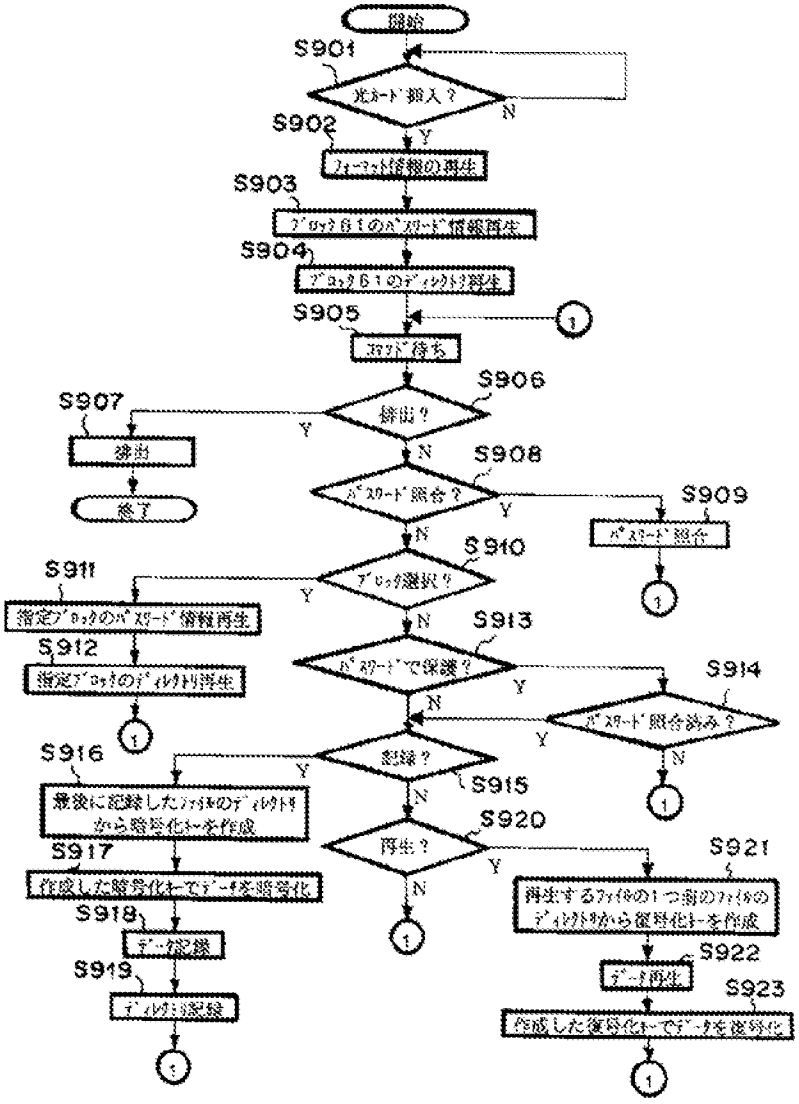
【図4】


62
61
F方向
B方向

【図8】


暗号化／復号化回路
42
36
ホストコンピュータ
32
MPU
33
40
41
Y
Z
30
38
39
34
AT／AF
制御回路
31
R
1
35
37
変調回路

【図9】


開始
S901
光ｶｰﾄﾞ挿入？
N
Y
S902
ﾌｫｰﾏｯﾄ情報の再生
S903
ﾌﾞﾛｯｸ毎のﾊﾟｽﾜｰﾄﾞ情報再生
S904
ﾌﾞﾛｯｸ毎のﾃﾞｨﾚｸﾄﾘ再生
S905
ｺﾏﾝﾄﾞ待ち
S906
排出？
S907
排出
終了
S908
ﾊﾟｽﾜｰﾄﾞ照合？
S909
ﾊﾟｽﾜｰﾄﾞ照合
S910
ﾌﾞﾛｯｸ選択？
S911
指定ﾌﾞﾛｯｸのﾊﾟｽﾜｰﾄﾞ情報再生
S912
指定ﾌﾞﾛｯｸのﾃﾞｨﾚｸﾄﾘ再生
S913
ﾊﾟｽﾜｰﾄﾞで保護？
S914
ﾊﾟｽﾜｰﾄﾞ照合済み？
S915
記録？
S916
最後に記録したﾌｧｲﾙのﾃﾞｨﾚｸﾄﾘから暗号化ｷｰを作成
S917
作成した暗号化ｷｰでﾃﾞｰﾀを暗号化
S918
ﾃﾞｰﾀ記録
S919
ﾃﾞｨﾚｸﾄﾘ記録
S920
再生？
S921
再生するﾌｧｲﾙの1つ前のﾌｧｲﾙのﾃﾞｨﾚｸﾄﾘから復号化ｷｰを作成
S922
ﾃﾞｰﾀ再生
S923
作成した復号化ｷｰでﾃﾞｰﾀを復号化